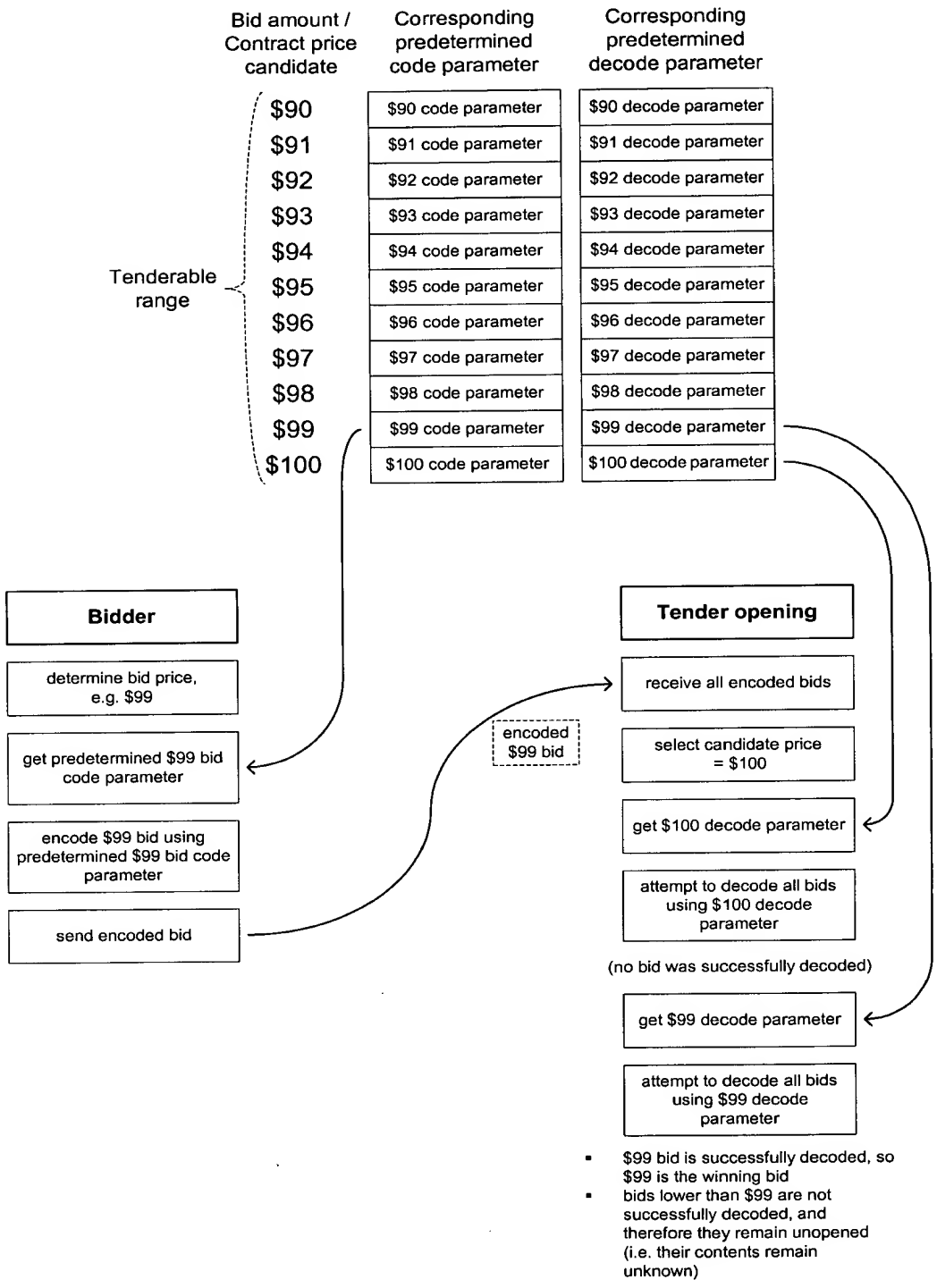
Claimed invention

The claimed invention is directed to an electronic system used for purposes such as auctions, in which several bids are received, and one bid is chosen as the winning bid because it is either the highest or lowest bid (depending on the type of auction). A goal of the claimed invention is to determine which bid is the winning bid without opening all of the bids, thereby preserving the anonymity of the non-winning bidders and the amounts of their bids.

The features of the claimed system are illustrated in the following figure:


Bid amount / Contract price candidate
Corresponding predetermined code parameter
Corresponding predetermined decode parameter
Tenderable range
$90
$91
$92
$93
$94
$95
$96
$97
$98
$99
$100
$90 code parameter
$91 code parameter
$92 code parameter
$93 code parameter
$94 code parameter
$95 code parameter
$96 code parameter
$97 code parameter
$98 code parameter
$99 code parameter
$100 code parameter
$90 decode parameter
$91 decode parameter
$92 decode parameter
$93 decode parameter
$94 decode parameter
$95 decode parameter
$96 decode parameter
$97 decode parameter
$98 decode parameter
$99 decode parameter
$100 decode parameter
Bidder
determine bid price, e.g. $99
get predetermined $99 bid code parameter
encode $99 bid using predetermined $99 bid code parameter
send encoded bid
encoded $99 bid
Tender opening
receive all encoded bids
select candidate price = $100
get $100 decode parameter
attempt to decode all bids using $100 decode parameter
(no bid was successfully decoded)
get $99 decode parameter
attempt to decode all bids using $99 decode parameter
$99 bid is successfully decoded, so $99 is the winning bid
bids lower than $99 are not successfully decoded, and therefore they remain unopened (i.e. their contents remain unknown)

In the claimed system as illustrated above, for each possible bid within a "tenderable range" (the range between the minimum and maximum bid), there is a corresponding, predetermined "code parameter" that is used for encoding a bid of that amount. In other words, a $99 bid is encoded using the $99 code parameter, whereas a $95 bid is encoded using the $95 code parameter.

Each bid in the tenderable range also has a corresponding, predetermined "decode parameter" that is used to decode bids that have been encoded using the code parameter for that same amount. In other words, a $99 bid is encoded using the $99 code parameter, and so it can only be decoded using the corresponding $99 decode parameter.

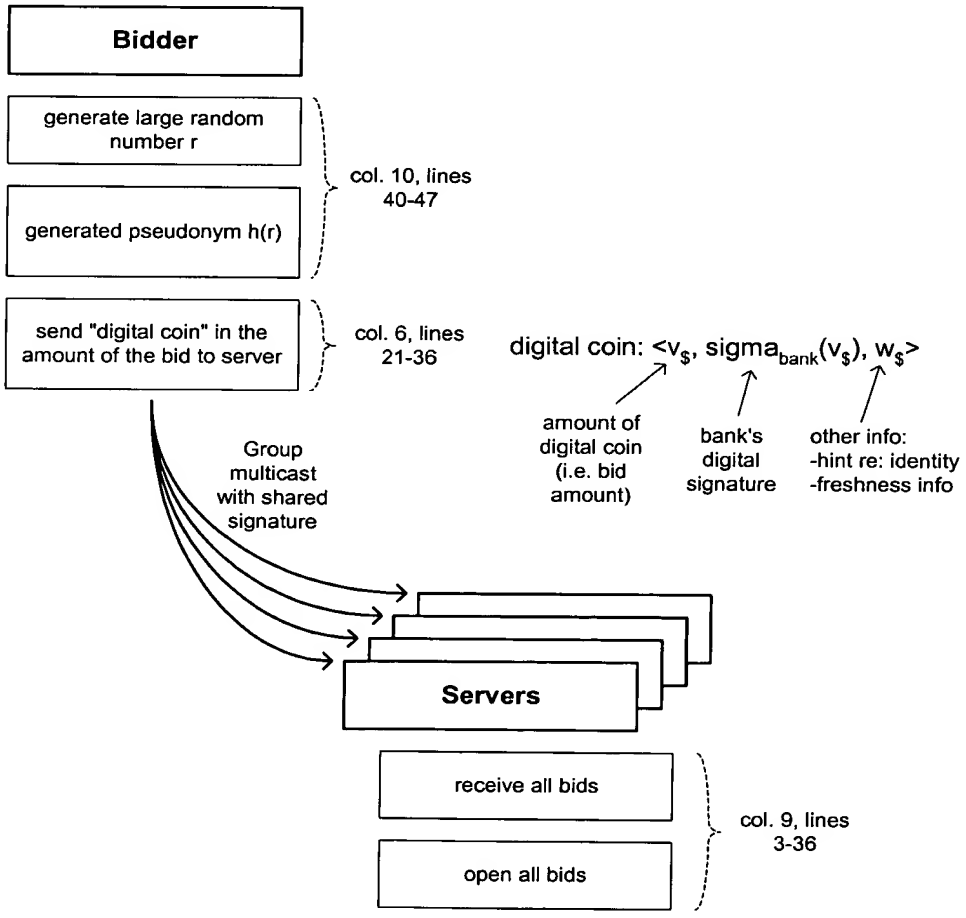
Therefore the code parameters and decode parameters have two important features: they are *predetermined*, meaning that they are defined prior to and separately from the auction; and, they *correspond to respective bid amounts*, meaning that each bid amount is associated with its own unique code and decode parameters. These features are shown at the top of the drawings.

The code and decode parameters are used in the manner shown in the bottom of the illustration. When a bidder has determined a bid price, e.g. $99, it gets the code parameter that corresponds to $99, and encodes its $99 bid using the $99 code parameter. This bid is then sent to a "tender opening sub-system" (server) that receives all bids from all bidders. Each received bid has been encoded by the respective bidder using the code parameter corresponding to the amount of the bid. At the server, once all bids have been received, the server begins a process of attempting to decode all of the received bids, starting with the decode parameter for the highest (or lowest) possible bid, and working down (or up) until it is finally able to decode a bid. For example, in the illustration, the server is seeking to identify the highest bid. It begins by trying to decode every received bid using the $100 decode parameter. For this example, it is assumed that no one has bid $100. In that case, none of the received bids have been encoded using the $100 code parameter, and so none of the bids can be decoded using the $100 decode parameter. Therefore, by attempting and failing to open any bid using the $100 decode parameter, the

server determines that there is no $100 bid without revealing the contents of any of the bids. The server then gets the decode parameter for the next lowest bid, $99, and tries again to decode all bids, this time using the $99 decode parameter. In the present example, the server will successfully decode the $99 bid using the $99 decode parameter. The server therefore decodes the highest bid, while the other remaining bids are not decoded, and so their contents are not revealed. These features are shown at the bottom of the drawing.

The features shown in the illustration and described above are recited in the present independent claims. It is believed that by reading the claims side-by-side with the illustration above, all of the features of the claims will be easily recognized in the illustration.

The Franklin system is significantly different than the system presently claimed. The following illustration shows Franklin's basic system:



Franklin submits bids in the form of a "digital coin," which is a form of electronic money that Franklin describes at col. 6, lines 21-36. The bidder may avoid disclosing his identity by using a pseudonym generated from a random number. A piece of each bid is transmitted to a different server through a group multicast process, as described at col. 4, line 18 - col. 5, line 64, and at col. 8, line 47 - col. 9, line 2. The pieces of the bids are received by the respective servers, and those pieces are shared to reconstruct each bid, as described at col. 9, lines 3-21. Bids determined to be invalid through this process are discarded. All bids are then opened and consistency among the portions is inspected, as described at col. 9, lines 22-36. Bids determined to be invalid through this process are also discarded. The validity of the "digital coin" contained in each bid is then confirmed, as explained at col. 9, lines 7-53. While Franklin's system is complex, it is sufficient for present purposes to recognize that Franklin validates bids using multicast, public and private keys, and digital coins, and that this process involves opening all bids.

Franklin is significantly different than the claimed invention. In the claimed invention, the manner in which a bid is encoded is determined by the value of the bid -- specifically, the bid is encoded using a predetermined code parameter that corresponds to the bid value. Franklin does not have predetermined code parameters that correspond to bid values. Instead, Franklin encodes bids using public and private keys that are specific to the bidder, provides further validation through multicast to multiple servers and through digital coins having their own validation schemes. Franklin does not encode bids using code parameters that are predetermined and specific to the value of the bid that is being encoded. Consequently, Franklin's decoding does not involve getting decode parameters that are specific to bid amounts, and then attempting to decode each bid using decode parameters corresponding to successive bid amounts until a bid is finally successfully decoded.

The present claims are directed to the features of a system that includes a bidding device and a server (claims 1-8), the method performed in the bidding device (claim 9), and the method performed in the server (claim 10). Each set of claims includes features as described above that are not found in Franklin. It

is believed that Franklin is significantly different than the claimed invention and does not anticipate or make obvious the claimed invention. Therefore allowance of all claims is appropriate at this time.

The foregoing amendments and remarks address all bases for rejection and are believed to place the case in condition for allowance. The examiner is invited to contact the undersigned to resolve any remaining issues.

Respectfully submitted,

Date: July 23, 2003

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

Ronald Coslick
Registration No. 36,489